Matematiska Institutionen
KTH

Solutions to the exam to Discrete Mathematics, SF2736, December 14, 2012, 08.00–13.00.

Examiner: Olof Heden

Observe:

1. You are not allowed to use anything else than pencils, rubber, rulers and papers at this exam.
2. To get the maximum number of points on a problem it is not sufficient to just give an answer, you must also provide explanations.
3. Bonus points from the homeworks will be added to the sum of the points on part I.
4. Grade limits: 13-14 points will give an Fx; 15-17 points will give an E; 18-21 points will give a D; 22-27 points will give a C; 28-31 points will give a B; 32-37 points will give an A.

Part I

1. (3p) Solve, by using the technique with generating functions, the recursion

$$a_0 = 2, \quad a_1 = 2, \quad \text{and,} \quad a_n = 2a_{n-1} + 8a_{n-2}, \quad \text{for} \quad n = 2, 3, \ldots .$$

Solution. Let $A(t) = \sum_{n=0}^{\infty} a_n t^n$. As

$$a_n t^n = 2ta_{n-1}t^{n-1} + 8t^2 a_{n-2} t^{n-2}$$

for $n = 2, 3, \ldots$ we get by adding these equalities that

$$A(t) - a_1 t - a_0 = 2t(A(t) - a_0) + 8t^2 A(t).$$

We simplify this to

$$A(t) = \frac{2 - 2t}{1 - 2t - 8t^2},$$

and by partial fractions

$$A(t) = \frac{2 - 2t}{(1 + 2t)(1 - 4t)} = \frac{1}{1 + 2t} + \frac{1}{1 - 4t}.$$

Expanding in geometric series gives

$$A(t) = \sum_{n=0}^{\infty}(-2t)^n + \sum_{n=0}^{\infty}(4t)^n = \sum_{n=0}^{\infty}((-2)^n + 4n)t^n,$$

and hence,

Answer: $a_n = (-2)^n + 4^n$.

2. (a) (1.5p) Find $5^{255}(\text{mod } 127)$.

   Solution. We find that 127 is a prime number, so we can use the Fermat theorem and get

   $$5^{255} \equiv_{127} 5^{2\cdot 126+3} \equiv_{127} (5^{126})^2 5^3 \equiv_{127} 1^2 5^3 \equiv_{127} 125.$$

   Answer: 125.

   (b) (1.5p) Find $5^{255}(\text{mod } 129)$.

   Solution. As $129 = 3 \cdot 43$ we get that for the Euler φ-function

   $$\varphi(129) = 3 \cdot 143(1 - \frac{1}{3})(1 - \frac{1}{43}) = 84.$$

   Hence by the theorem of Euler

   $$5^{255} \equiv_{129} 5^{3\cdot 84+3} \equiv_{129} (5^{84})^3 5^3 \equiv_{129} 1^3 5^3 \equiv_{129} 125.$$

   Answer: 125.

3. (3p) There are four classes in a school, each consisting of 15 children. A committee consisting of 12 children shall be chosen. In how many ways can this be done if it is required that the committee must have at least one child from each class.

   Solution. The classes are defined by the students that attend the classes and thus labeled. We give them the labels 1, 2, 3 and 4. Let B_i denote the set of committees that do not contain any member from class number i, for $i = 1, 2, 3, 4$. Then, as there are in total 60 students in the school we get that the number of committees will be

   $$\binom{60}{12} - |B_1 \cup B_2 \cup B_3 \cup B_4|.$$

   We will use the principle of inclusion and exclusion and for that purpose we calculate

   $$|B_i| = \binom{45}{12}, \qquad |B_i \cap B_j| = \binom{30}{12} \qquad |B_i \cap B_j \cap B_k| = \binom{15}{12}.$$

   Hence, as there are 6 possibilities to choose a subset $\{i, j\}$ of size two to the set $\{1, 2, 3, 4\}$ and 4 possibilities to choose a subset $\{i, j, k\}$ of size three to the set $\{1, 2, 3, 4\}$

   Answer:

   $$\binom{60}{12} - 4\binom{45}{12} + 6\binom{30}{12} - 4\binom{15}{12}.$$

4. Let G denote the group which is the following direct product of the groups $(Z_3, +)$ and $(Z_2, +)$:

$$G = (Z_3, +) \times (Z_2, +) \times (Z_2, +) \times (Z_2, +).$$

(a) (1.5p) Find one subgroup of size six to G.

Solution.
Answer: The group $(Z_3, +) \times (Z_2, +) \times \{0\} \times \{0\}$ contains six elements.

(b) (1.5p) Find the number of distinct subgroups of size six to G.

Solution. By considering the different orders of the elements in the given group we find that there are exactly 14 distinct "words" of order six, namely

$$(1, 1, 0, 0),\ (1, 0, 1, 0),\ (1, 0, 0, 1),\ (1, 0, 1, 1),\ (1, 1, 0, 1),\ (1, 1, 1, 0),\ (1, 1, 1, 1).$$

and

$$(2, 1, 0, 0),\ (2, 0, 1, 0),\ (2, 0, 0, 1),\ (2, 0, 1, 1),\ (2, 1, 0, 1),\ (2, 1, 1, 0),\ (2, 1, 1, 1).$$

Each of these 14 elements generate a subgroup of size six. However,

$$< (1, x, y, z) >=< (2, x, y, z) >$$

for all $(x, y, z) \in (Z_2, +) \times (Z_2, +) \times (Z_2, +) \setminus \{(0.0.0)\}$.
As every abelian group of size six is cyclic, and as every subgroup of an abelian group, which the given group is, is an abelian group we thus get
Answer: Seven.

5. Let G be a graph, with no loops and no multiple edges, with 1024 edges and 1024 vertices. Answer the following two question together with a short explanation.

(a) (1p) If G is connected then G has at least one cycle. Why?

Solution. If the given graph with 1024 vertices and 1024 vertices had no cycles, as being connected it would be a tree. However, a tree on 1024 vertices has 1023 edges. Hence the graph has at least one cycle.
Answer:

(b) (2p) If G consists of two components, which are then the possibilities for the number of cycles in G?

Solution. We will use the fact that a connected graph G' with v vertices and v edges has exactly one cycle, a fact that we prove first (you will not get your number of points reduced if you take this fact for granted): We know from previous subproblem that the graph G' has at least one cycle. Delete the edge e between the vertices a_1 and a_2 in a cycle in G'. The remaining graph is connected, and since it have $v - 1$ edges it is a tree T. Then, between the vertices a_1 and a_2 there is exactly one path in T, as if there were two paths, they could be combined to a cycle.

Now back to the given problem. Assume that one of the components contain x vertices and x edges and the other component $1024 - x$ vertices and $1024 - x$ edges. Then each component has exactly one cycle, so in this case there are two cycles in the graph.

A connected graph on x vertices must have at least $x - 1$ edges, (as it as a subgraph has a spanning tree). So the other case is when one component is a tree T_1 on x vertices with no cycles, and the other component is a connect graph G_1 with $1024 - x$ vertices and $1024 - x + 1$ edges, and thus has at least one cycle C_1. Delete the edge e in that cycle. We then get a graph G_2 which is connected and according to the facts first proved, has exactly one cycle C_2

$$a_1 e_1 a_2 e_2 a_3 \cdots a_\ell e_\ell a_1,$$

with vertices a_i and edges e_i for $i = 1, 2, \ldots, \ell$. If the deleted edge e did not incidence with any of the vertices a_i, for $i = 1, 2, \ldots, \ell$, then the graph G_1 has just the two cycles C_1 and C_2. In case e is incident with exactly one of the vertices in the cycle C_2, then G_1 have two or three cycles, depending on whether C_1 and C_2 has none or more edges in common, respectively, as if they have an common edge then we can produce three cycles, in a way similar to how it is done below. If e is incident with two vertices a_i and a_j in the cycle C_2, then G_1 has three cycles, the cycle C_2 and the cycles

$$a_1 e_1 a_2 e_2 a_3 \cdots e_{i-1} a_i e a_j e_j \cdots a_\ell e_\ell a_1, \quad \text{and} \quad a_i e_i a_{i+1} e_{i+1} a_{i+2} \cdots a_{j-1} e_{j-1} a_j e a_i.$$

Answer: Two or three cycles.

Part II

6. (3p) Are there any permutations φ, ψ and δ in the symmetrical group $\mathcal{S}_{12}$, the group consisting of all permutations on the set $\{1, 2, \ldots, 12\}$, such that

$$\varphi^4 = (1\ 2)(3\ 4)(5\ 6), \qquad \psi^5 = (1\ 2)(3\ 4)(5\ 6), \quad \text{and} \quad \delta^6 = (1\ 2)(3\ 4)(5\ 6).$$

Solution. Take $\psi = (1\ 2)(3\ 4)(5\ 6)$, then as for every 2-cycle $(a\ b)$, it is true that $(a\ b)(a\ b) = \text{id}$. we get that $(a\ b)^5 = (a\ b)$ and thus that $\psi^5 = \psi$, that is, yes ψ exist.

If φ exist, then, as every 2-cycle has order 2, we may conclude that $\varphi^8 = \text{id.}$. It follows that the order of φ must be a divisor of 8, and thus indeed equal to 8 as else $\varphi^4 = \text{id.}$. One of the cycles in the cycle decomposition of φ then must have length 8. If you raise a cycle of length 8 to the power 4 you get a product of four 2-cycles. But φ shall be a product of three 2-cycles. Thus φ does not exist.

We treat δ similarly, as we get that $\delta^{12} = \text{id.}$ and thus that δ must be a product of cycles of lengths in the set $\{1, 2, 3, 4, 6, 12\}$. Arguing as above, we get that no cycle can have length 12, and a cycle of length 6, when raised to the power 6 will give just the identity. So for δ to have the order 12, at lest one cycle must have order 4 and one cycle must have order 3. Cycles of the lengths 2 or 3 raised to the power six gives the identity, and a cycle of length 4 raised to the power six gives a product of two 2-cycles. Three 2-cycles can never occur as a product of a family of mutually disjoint pair of 2-cycles. Thus, δ do not exist.

Answer: Just ψ exist, E.G. $\psi = (1\ 2)(3\ 4)(5\ 6)$.

7. (4p) Find the number of surjective maps f from the set $A = \{1, 2, \ldots, 9\}$ to the set $\{1, 2, \ldots, 5\}$ such that

$$|\{x \in A \mid f(x) = f(1)\}| = |\{x \in A \mid f(x) = f(2)\}|.$$

Besides explanations, your answer to this question must be given as a product and sum of integers.

Solution. We divide into distinct cases.

Case 1. $|\{x \in A \mid f(x) = f(1)\}| = 1$. Then $f(1) \neq f(2)$, so we have to divide the remaining $9 - 2 = 7$ elements into 3 distinct unlabeled bags which can be done in $\mathrm{S}(7, 3)$ distinct ways. Then we must label the in total five bags, of which two contains the elements 1 and 2, respectively. That can be done in 5! ways. Hence this case contributes with $5! \cdot \mathrm{S}(7, 3)$ surjective maps.

Case 2. $|\{x \in A \mid f(x) = f(1)\}| = 2$. There are then two subcases, The first is when $f(1) = f(2)$. Then the remaining seven elements must be partitioned into 4 unlabeled bags. Else as in the previous case. Hence this subcase contributes with $5! \cdot \mathrm{S}(7, 4)$ surjective maps. In the other subcase, we have $f(1) \neq f(2)$, and we must choose elements in the set $\{3, 4, \ldots, 9\}$ that go to the same bag as the elements 1 and 2, respectively. They can be chosen in $7 \cdot 6$ ways. It remains 5 elements that shall go to 3 distinct bags, and after that we label the bags in 5! ways. So this subcase contributes with $5! \cdot 7 \cdot 6 \cdot \mathrm{S}(5, 3)$ surjective maps.

Case 3. $|\{x \in A \mid f(x) = f(1)\}| = 3$. As in previous case there are two subcases. In the first of these subcases we have $f(1) = f(2)$. We choose one element to go to the same bag as the elements 1 and 2, which can be done in 7 distinct ways. As above we get $7 \cdot 5! \cdot \mathrm{S}(6, 4)$ surjective maps. In the other subcase we have $f(1) \neq f(2)$ and hence in total

$$\binom{7}{2}\binom{5}{2}5!\mathrm{S}(3, 3)$$

surjective maps.

Case 4. $|\{x \in A \mid f(x) = f(1)\}| = i$, for $i = 4, 5$. In this case just one possibility appear, $f(1) = f(2)$ and, like in the solutions above, we get

$$\binom{7}{i-2}5!\mathrm{S}(9 - i, 4)$$

surjective maps.

It remains to calculate the Stirling numbers, whereby we use the recursion

$$\mathrm{S}(n, k) = \mathrm{S}(n - 1, k - 1) + k\mathrm{S}(n - 1, k).$$

Trivially $S(4,4) = S(3,3) = 1$. As $S(n, n-1) = \binom{n}{2}$ we get that $S(5,4) = 10$. We continue

$$S(5,3) = S(4,2) + 3S(4,3) = 7 + 3\binom{4}{2} = 25,$$

and

$$S(6,4) = S(5,3) + 4S(5,4) = 25 + 4 \cdot 10 = 65.$$

and

$$S(7,3) = S(6,2) + 3S(6,3) = S(5,1) + 2S(5,2) + 3(S(5,2) + 3S(5,3)),$$

and $S(6,3) = 65$. But

$$S(5,2) = S(4,1) + 2S(4,2) = 1 + 2 \cdot 7 = 15,$$

so

$$S(7,3) = 1 + 2 \cdot 15 + 3(15 + 3 \cdot 25) = 301.$$

Finally,

$$S(7,4) = S(6,3) + 4S(6,4) = 90 + 4 \cdot 65 = 350.$$

Answer:

$$5!(301 + 350 + 42 \cdot 25 + 210 + 21 \cdot 10 + 35),$$

(which can be calculated to 226320.)

8. Let C denote the set of words $(c_1, c_2, \ldots, c_{11})$ in $Z_2^{11} = Z_2 \times Z_2 \times \cdots \times Z_2$ such that

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_{11} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

The code C is an 1-error-correcting code (you do not need to prove this fact!).

(a) (1p) Correct the word $(0,0,0,0,1,1,1,0,0,0,0)$.

Solution. We get that

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \left(\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right) = \left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

and thus,

Answer: $(0,0,0,1,1,1,1,0,0,0,0)$

(b) (1p) Find a word that cannot be corrected.

Solution. Denote the 11×4-matrix above by $\mathbf{H}$. A word $\bar{c}$ can be corrected if there is a column $\bar{k}$ in the matrix $\mathbf{H}$ such that

$$\mathbf{H}\bar{c}^T + \bar{k} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

So we consider the set of columns we get when we add the column $[1\ 0\ 1\ 1]^T$ to the set of columns. For example we find that the column $[0\ 1\ 0\ 0]^T$ does not occur, as the column $[1\ 1\ 1\ 1]^T$ is not among the columns of $\mathbf{H}$. Thus, a word $\bar{x}$ such that

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} (\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix})$$

cannot be corrected. It is easy to find such word, take for example

$$\bar{x} = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0],$$

which is our :**Answer**

(c) (1p) How many words cannot be corrected?

Solution. Let $\bar{d} = [1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0]$. Then

$$\mathbf{H}\bar{d}^T = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix},$$

and hence

$$\mathbf{H}\bar{c}^T = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \Longleftrightarrow \qquad \mathbf{H}(\bar{c}^T + \bar{d}^T) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix},$$

so the words of the given code C are in $1-1$-correspondence with the words in the null space of $\mathbf{H}$. Hence

$$|C| = 2^{n-\mathrm{rank}(\mathbf{H})} = 2^{11-4} = 128$$

Still the words at distance one from a code word are those that can be corrected, so every code word $\bar{c}$ can correct 12 words, inclusively the word $\bar{c}$. The number of words that cannot be corrected is thus equal to

$$2^n - |C|(1+n) = 2^{11} - 2^7 \cdot 12 = 2^{11} - 3 \cdot 2^9 = 2^9 = 512.$$

Answer: 512

(d) (2p) Let $\bar{c}^T$ denote the transpose of a matrix $\bar{c}$. If the first column in the 4×11-matrix above is substituted by the column $[0\ 0\ 0\ 0]^T$, $[0\ 0\ 1\ 1]^T$, or $[1\ 0\ 1\ 1]$, then the matrix equation above gives, instead of C, three other codes C_1, C_2 and C_3, respectively. Are any of these three codes an 1-error-correcting code?

Solution. Let $\bar{e}_i$ denote the word of weight one with it single non zero position i. If we substitute the first column with $[0\ 0\ 0\ 0]^T$ and find a word $\bar{c}$ in that code, then also $\bar{c} + \bar{e}_1$ will belong to C, so minimum distance cannot be three. Siimilarly for the substitution by $[0\ 0\ 1\ 1]^T$, then for every code word $\bar{c}$, also the word $\bar{c} + \bar{e}_1 + \bar{e}_2$ will belong o C and minimum distance will be 2.
If we substitute by $[1\ 0\ 1\ 1]^T$, then the code C we get is the coset $\bar{d} + C_0$ (where $\bar{d}$ is as in previous subproblem) of the null space C_0 of that new matrix. This new matrix has mutually distinct non-zero columns and thus C_0 is an 1-error-correcting code with minimum distance three. Using the fact that

$$\mathrm{d}(\bar{d} + \bar{c}, \bar{d} + \bar{c}') = \mathrm{w}(\bar{d} + \bar{c} - \bar{d} - \bar{c}') = \mathrm{w}(\bar{c} - \bar{c}') \geq 3$$

for any two words $\bar{c}$ and $\bar{c}'$ of C_0, we get that the minimum distance in C is three.

Answer: Just the substitution by $[1\ 0\ 1\ 1]^T$ gives an 1-error-correcting code.

Part III

9. (5p) Let G be a bipartite graph with the two sets of vertices X and Y of the same size. (No edge between any two vertices in X and similarly for Y.) For any subset A of X and any subset B of Y let

$$R(A) = \{y \in Y \mid y \text{ is neighbor to at least one } x \in A\},$$

$$L(B) = \{x \in X \mid x \text{ is neighbor to at least one } y \in B\}.$$

Show that there is a subset A of X such that $|A| > |R(A)|$ if and only if there is at least one subset B of Y such that $|B| > |L(B)|$.

Solution. If there is no subset B of Y such that $|B| > |L(B)|$ then there is, by the marriage theorem of Hall, a complete matching in the given graph where every y in Y is matched to an x in X. As X and Y have the same number of elements, this matching also is a matching where every vertex in X is matched to a vertex in Y. Then, for every subset A of X, it must be true that $|A| \leq |R(A)|$.

If there is a subset B of Y such $|B| > |L(B)|$ then there cannot be a complete matching where every y in Y is matched to a vertex x in X. Again, as X and Y have the same number of elements, there is no complete matching where every vertex in X is matched to a vertex in Y. Hence, again by the marriage theorem of Hall, there must be a subset A of X such that $|A| > |R(A)|$.

Answer:

10. (5p) Let a, b and d be elements in a ring Z_n. Find the number of solutions x and y in Z_n to the equation

$$ax + by = d.$$

(Partial solutions to this problem will give one or more points, for example you will get 1p if you solve the problem in the case $\gcd(a, n) = 1$.)

Solution. In case a (or b) are coprime to n there are exactly n distinct solutions to each d as then, for each $y \in Z_2^n$,

$$ax + by = d \qquad \Longleftrightarrow \qquad x = a^{-1}(d - by).$$

Now let $D_a = \gcd(a, n)$ and $D_b = \gcd(b, n) = D_b$ and let $D = \gcd(D_a, D_b)$, in fact $D = \gcd(a, b, n)$. Then, $ax = D_a - kn$ has an integer solution (x, k) and thus $D_a \in < a >$. Furthermore D_a divides a, $a = k' D_a$, so $a \in < D_a >$. Thus

$$< a >=< D_a >, \qquad \text{and} \qquad < b >=< D_b > .$$

The given equation has a solution if and only if d belongs to the additive subgroup G of $(Z_n, +)$ generated by the elements a and b, which is the smallest subgroup containing both a and b. In fact

$$G =< D >,$$

as every multiple of D is in G and as both a and b are multiples of D,

$$a = k_1 D_a = k_a D, \quad b = k_2 D_b = k_b D, \quad \Rightarrow \quad ax + by = (xk_a + yk_b)D,$$

so no other elements than multiples of D appear in G. Furthermore D divides n.

So now we count the number of solutions when $d \in < D >$.

Without loss of generality we can assume that $a = D_a$ and that $b = D_b$ as $< a >=< D_a >$ and similarly for b. Assume that

$$d = D_a x + D_b y = D_a x' + D_b y'.$$

Then

$$D_a(x - x') = D_b(y' - y) \in < D_a > \cap < D_b > . \tag{1}$$

Let m denote the least common multiple of D_a and D_b. As both D_a and D_b divides n we get, by the definition of the least common multiple, that m divides n and that every element divisible by both D_a and D_b is divisible by m. Hence

$$< D_a > \cap < D_b >=< m > .$$

The number of elements in $< m >$ is n/m, indeed

$$< m > = \{m, 2m, \ldots, \frac{n}{m}m = 0\},$$

and similarly for the other cyclic groups discussed above. We can thus conclude from Equation (1) above that

$$D_a(x - x' + \mu\frac{n}{D_a}) = \lambda m,$$

for each $\mu \in \{0, 1, 2, \ldots, D_a\}$ and some $\lambda \in \{1, 2, \ldots, \frac{n}{m}\}$ or equivalently for each $\lambda = 1, 2, \ldots, n/m$

$$x = x' + \mu_x\frac{n}{D_a} + \lambda\frac{m}{D_a}, \qquad \mu_x = 0, 1, 2, \ldots, D_a$$

and, again from Equation (1),

$$y = -y' + \mu_y\frac{n}{D_b} - \lambda\frac{m}{D_b}, \qquad \mu_y = 0, 1, 2, \ldots, D_b$$

It is easy to check that for each such λ and every possible combination of μ_x and μ_y, in the given sets above, we get a solution. Hence, in case $d \in < D >$ the number of solutions is

$$\frac{n}{m}D_aD_b$$

which is equal to

$$\frac{n\mathrm{gcd}(a,n)\mathrm{gcd}(b,n)}{\mathrm{lcm}(\mathrm{gcd}(a,n),\mathrm{gcd}(b,n))} = \frac{n\mathrm{gcd}(a,n)\mathrm{gcd}(b,n)}{\frac{\mathrm{gcd}(a,n)\mathrm{gcd}(b,n)}{\mathrm{gcd}(\mathrm{gcd}(a,n),\mathrm{gcd}(b,n))}} =$$

$$= n\mathrm{gcd}(\mathrm{gcd}(a,n),\mathrm{gcd}(b,n)) = n\mathrm{gcd}(a,b,n)$$

We thus get the

Answer: Let $D = \mathrm{gcd}(a, b, n)$. If $d \in < D >$, that is, is a multiple of the greatest common divisor of a, b and n, then the number of solutions to the given equation is nD. If $d \notin < D >$ then there are no solutions.